CLAIMS

1. A method of communicating an electronic document between security domains, the method comprising the steps of:

receiving, in a first security domain, a request to transmit to a second security domain a first electronic document in a first data format capable of supporting one or more (covert) security threats;

creating a second document in a second data format incapable of supporting the one or more security threats, responsive to the content of the first document;

forwarding the second document in place of the first document to the second security domain.

2. A method according to any preceding claim in which forwarding of the second document is conditional upon user sanction.

3. A method according to any preceding claim in which the second document is digitally signed by a sanctioning user.

4. A method according to any preceding claim in which the second document is forwarded to the second security domain via at least one data diode.

5. A method according to any preceding claim in which the step of creating the second document comprises performing a transformation to the first document which modifies the underlying data format of the document whilst substantially preserving the visible informational content.

6. A method according to any preceding claim in which the step of creating the second document comprises adding at least one of entropy and randomness to at least one characteristic of the representation of the first document.

7. A method according to claim 6 in which the at least one characteristic comprises at least one of colour and spacing.

8. A method according to any preceding claim in which the step of creating the second document comprises applying a lossy compression method.

9. A method according to any preceding claim comprising the step of:

conveying the second document to a user sanction function for review and sanction prior to sending the second document to the second security domain.

10. A method according to any preceding claim in which review and sanction comprises sanction by a human user.

11. A method according to any preceding claim in which the one or more security threats comprise presence in the first document of malicious code.

12. A method according to claim 11 in which the malicious code comprises at least one of a computer virus and a Trojan horse.

13. A method according to any preceding claims in which the one or more security threats comprises data steganographically concealed within the first document.

14. A method according to any preceding claim in which the first security domain and second security domain are rated at different security levels.

15. A method according to any preceding claim in which the first security domain is a lower-level security domain than the second security domain.

16. A method according to any one of claim 1-14 in which the first security domain is a higher-level security domain than the second security domain.

17. A method of communicating an electronic document between security domains, substantially as described in the foregoing description and/or with reference to the accompanying figures.

18. Apparatus arranged to perform the methods of any one of claims 1-17.

19. A computer system arranged to perform the methods on any one of claims 1-17.

20 A computer chipset arranged to perform the methods on any one of claims 1-17.

21. A program for a computer comprising code portions arranged to perform the methods on any one of claims 1-17.